REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-19 are currently pending in this application and Claims 1, 7, 13, 14 and 18 are amended.

In the outstanding Office Action claims 1-19 were rejected under 35 U.S.C. §103(a) as unpatentable over Takashima et al. (U.S. Patent No. 5,701,343, hereinafter Takashima).

Support for the amendments to Claims 1, 7, 13 and 14 can be found in the Specification at page 9, lines 25-33 and at page 14, line 30 to page 15, line 12, for example, and therefore, Applicants respectfully submit that no new matter is added. The amendment to Claim 18 changes the dependency from Claim 1 to Claim 14, and therefore, no new matter is added.

Amended Claim 1 is directed toward a program distribution device for distributing executable programs through a network to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance. The program distribution device includes a first communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor. The first and second communication paths are set up as different channels on an identical transmission line or as different transmission lines. An encryption processing unit is configured to produce an encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor. A transmission unit is configured to transmit the encrypted program to the tamper resistant processor through the second communication path, so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted

program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key. This configuration allows program distribution to occur directly between a program distribution device and a microprocessor safely and efficiently without intervention by a third party.[1]

With respect to the rejection of Claim 1, Applicants respectfully traverse the outstanding rejection because Takashima fails to make obvious amended Claim 1. Claim 1 has been amended to recite "...directly connecting the program distribution device and the tamper resistant processor, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines...." Indeed, Takashima does not teach, suggest or make obvious this element of amended Claim 1.

Takashima only discloses connecting an information center and an information terminal device through a communications network,[2] and connecting a computer card to an information terminal device connected to the information center.[3] Takashima does not discuss connecting the computer card to the information center. Thus, Takashima does not teach, suggest or make obvious the claimed "directly connecting the program distribution device and the tamper resistant processor, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines."

Claim 1 is also amended to recite "...executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor..." and "...the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key." Indeed, Takashima does not disclose or make obvious these elements of amended Claim 1.

---

[1] Specification, page 19, lines 6-14.
[2] Takashima, col. 6, lines 27-31.
[3] Takashima, col. 3, lines 54-56.

On the contrary, Takashima discloses encrypting information by using a work key to obtain encrypted information to be delivered.[4] This work key is generated at the information center,[5] and it is not a unique public key of any entity. Consequently, Takashima fails to teach, suggest or make obvious the claimed "...executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor..." and "...the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key."

In view of the above noted distinctions, Applicants respectfully submit that Claim 1 (and its dependent Claims 2-6) patentably distinguish over Takashima. Claims 7, 13, and 14 are similar to Claim 1. Applicants respectfully submit that Claims 7, 13, and 14 (and their dependent Claims 8-12, 15-19) patentably distinguish over Takashima for at least the reasons given for Claim 1.

Consequently, in view of the above amendments and comments, it is respectfully submitted that the outstanding rejection is overcome and the pending claims are in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H.Kuesters
Attorney of Record
Registration No. 28,870

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JW\203058US\203058US_AM.DOC

[4] Takashima, col. 10, lines 38-46.
[5] Takashima, col. 10, lines 1-6.